



# Grant Thornton

An instinct for growth<sup>TM</sup>

## Information Commissioner's Office

### Internal Audit 2013-14: IT Contract Management review

Last updated 4 July 2014

Distribution		Timetable	
For action	Director of Corporate Services	Fieldwork completed	19 May 2014
For information	Head of IT	Draft report issued	23 May 2014
For information	Audit Committee	Management comments	27 May 2014
		Final report issued	28 May 2014

This report is confidential and is intended for use by the management and Directors of the ICO only. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our prior written consent. We do not accept responsibility for any reliance that third parties may place upon this report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred, arising out of or in connection with the use of this report, however such loss or damage is caused.

It is the responsibility solely of the ICO management to ensure that there are adequate arrangements in place in relation to risk management, governance and control.

# 1 Executive Summary

## 1.1 Background

In 2013 the ICO established a new set of IT service contracts with a number of new suppliers, replacing a single contract with Capita. In order to ensure the management of the related contracts is effective, the ICO needs to implement management controls over the delivery of services to the ICO and hold the suppliers to account, according to those contracts. Contract management and the management of suppliers is becoming a key management activity for the IT department. Resources are limited within the IT department and wider management team so management of the contracts needs to be efficient as well as effective.

The two major IT contracts are with Northgate, covering Infrastructure & Systems Management, and Application & Desktop Management. Northgate use sub-contractors to support some systems, however from an ICO perspective the services are covered under the contracts with Northgate.

There are two other main service providers. SCC provides three services to the ICO: hardware & software purchasing, software licensing and information security (including ad-hoc advice, consultancy on projects and provision of IT Health-checks). Danwood supply printing services and support, and maintain all of ICO's printer devices and photocopiers.

The objective of the review was to establish the extent to which third-party services are being delivered according to contractual requirements and so meet the ICO requirements.

## 1.2 Scope

Our review involved an assessment of the following risks:

- Operational and legal requirements are not being met.
- Definition of the following areas are unclear.
  - Services being provided including those relating to security, availability and service recovery.
  - Responsibilities and accountabilities of suppliers and ICO staff.
  - Software licensing arrangements
  - contract breach or the remedies established should such a breach occur
- Risks and rewards for either party are not defined and agreed.
- There are inadequate mechanisms for establishing, agreeing, implementing and paying for contractual changes.
- No review points (either time or event driven) have been built in to the contract, so preventing either party from re-negotiating costs or services.
- Provisions are not in place to allow for smooth transition from a current supplier to a new supplier.

Further details on responsibilities, approach and scope are included in Appendix A.

## 1.3 Overall assessment

We have made an overall assessment of our findings as:

Overall assessment	
We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.	Green

Please refer to appendix B for further information regarding our overall assessment and audit finding ratings.

## 1.4 Key findings

Risk / Process	High	Medium	Low	Imp
Operational and legal requirements	-	-	3	-
Contract definition	-	-	-	-
Risks and rewards	-	-	-	-
Contractual changes	-	-	-	-
Contract review points	-	-	1	-
Transition arrangements	-	1	-	-
<b>Total</b>	-	<b>1</b>	<b>4</b>	-

There is one Medium rated finding arising out of our review, relating to a number of deliverables still required (principally from Northgate) under the transition arrangements. ICO management is fully aware of these, and we highlight the issues to help ensure focus is not lost. Further details of our findings and recommendations are provided in Section 2.

## 1.5 Areas of control in line with expectations

- For management of the two main IT contracts, there are weekly Service Review meetings in place. Any issues which cannot be resolved are escalated to the monthly Service Review meeting. Actions are tracked and carried forward to the next meeting. Issues which cannot be resolved at the monthly meeting are escalated to the Quarterly Service Review meeting.
- Specific individual responsibilities have not been documented. However, the membership of the different meetings is appropriate any issues identified are assigned an owner, and are subsequently monitored until resolved.
- Although specific definitions or examples of what constitutes a contractual breach are not defined, processes are in place to deal with any breach and these are included within the contracts. We understand that if a breach was thought to have occurred, senior management together with the Contract Manager would discuss the event and agree whether or not this was a breach. Only then would the potential breach be discussed with the supplier.

- Software licensing is being managed by the ICO with support from SCC. A register of licences is maintained within a spreadsheet and licence agreements are held within an online document repository. SCC carried out a review of software licensing and identified some exceptions following the transition from the old supplier. Ownership has been established and any licensing issues have now been resolved (such as licences not in ICO's name that should have been, and a third party being named on an ICO-only licence agreement).
- The scale of the contracts and the nature of the work undertaken is not considered to be conducive to exploring options around shared risk and reward,. For the Northgate contracts, there is a service credit process in place that ensures Northgate performance is managed and credits against the service charge are applied to compensate for poor performance. This is part of the framework provision from Government Procurement Service which all public bodies are encouraged to use whenever possible.
- A contract change process is in place whereby a Contract Change Note (CCN) is drafted by the Contract Manager following discussions with the contractor and ICO management. These are then signed by senior representatives from both parties. While there have been changes to Northgate contracts (seven so far), it has not changed the service charge, which has remained constant from August 2013 until April 2014, which is the most recent invoice. This tends to indicate that the changes have not been significant enough to change the charges.

There has been one Contract Change Note in respect of the contract with SCC. This was to correct a mistake regarding the level of expenditure expected - the contract indicated the figures applied to the life of the contract, whereas they should have related to annual spend.

- The in-scope contracts were established in July 2013, the annual review point is in July 2014. The annual review will address the following areas:
  - Review of annual contractor performance
  - Any uplift of service charges within the boundaries set in the contract
  - Service levels and associated service credit mechanism and caps on service credits
  - Proposals (by either party) for change of contract
  - CCN creation for all small changes, such as those to the infrastructure that ensure records are up to date but do not necessarily change the contract itself.

### **1.6 Acknowledgement**

We would like to take this opportunity to thank the staff involved for their co-operation during this internal audit.

## 2 Detailed Findings

### 2.1 Operational and legal requirements

1.	Low	Use of sub-contractors
Finding and Implication	Proposed action	Agreed action (Date / Ownership)
<p>At the April 2014 quarterly meeting it was identified that Kainos (Northgate's sub-contractor the for case management system - Meridio) had a relationship with Prizm, who supply a facility to read documents (such as Word or Adobe documents) within CMEH. We understand Prizm had not been paid for software maintenance; Northgate were not aware of this. Northgate dealt with the issue once it was brought to their attention.</p> <p>Incidents are recorded by Northgate's Service Desk, and the ICO can then exchange information with the relevant sub-contractor directly, to facilitate a resolution. Any material actions required as a result of the incident are referred back to Northgate.</p> <p>The issue raises the question of whether Northgate have fully identified all sub-contractors to their sub-contractors within the contracts with the ICO, and whether those relationships are being managed appropriately. The contract does not make any provision for the responsibilities for managing such "second line" sub-contractors, and there may therefore be dependencies and so risks which have not been recognised.</p>	<p>ICO should ensure that Northgate have identified all "second line" sub-contractors in use by their own sub-contractors and confirm that the management arrangement in place appropriately ensure that systems or components remain supported.</p>	<p><i>Agreed action</i> Northgate has previously been asked and have confirmed that they have identified and have contracts in place with all sub-contractors. ICO has visibility as a part of the monthly reporting process of the work of some key suppliers: Eduserv, Kainos and Frontline, The Service Delivery Manager and Contracts Manager will ensure they review these monthly reports. The performance of subcontractors is a standing item on the ICO/Northgate Monthly Service Board Agenda.</p> <p>The Head of IT will ask Northgate for more details of the process they followed to satisfy themselves that their contracts with their sub-contractors were adequate to meet their contractual obligations with the ICO.</p> <p><i>Date Effective:</i> 30 June 2014</p> <p><i>Owner:</i> Head of IT</p>

1.	Low	Use of sub-contractors
----	-----	------------------------

  

Finding and Implication	Proposed action	Agreed action (Date / Ownership)
	ICO should also ensure that the arrangements in place for communication, commissioning work and agreeing scope of work from such "second line" sub-contractors are clearly understood, documented and can be monitored	<p><i>Agreed action</i> The ICO is satisfied that there are sufficient mechanisms in place to capture and be aware of changes to the service provided, including those by second line subcontractors. In particular, Northgate needs to notify ICO of changes in key sub-contractors or changes in people providing support. System changes and changes to software would be visible through the Change Control process.</p> <p><i>Date Effective:</i> 27 May 2014</p> <p><i>Owner:</i> Head of IT</p>

2.	Low	Formalising SCC meetings
----	-----	--------------------------

Finding and Implication	Proposed action	Agreed action (Date / Ownership)
Meetings with Northgate and Danwood are documented and actions tracked. For the SCC Security contract, the Security Manager has only met with the SCC Account Manager on one occasion since the start of the Contract in March/April 2013. There have been other meetings relating to software licences and security relates service charges, with SCC. However, the meetings with SCC tend to be informal, task focused and are not documented.	We recommend that the ICO establishes regular service review meetings with SCC (at least every six months) and such meetings should be documented to ensure that action points are logged and monitored for progress. These should be shared with the SCC Account Manager to ensure that both parties are clear on what was discussed and action plans that arose from those discussions.	<p><i>Agreed action</i> ICO will schedule a formal six monthly review with SCC to cover all ICO/SCC contracts</p> <p><i>Date Effective:</i> 31 July 2014</p> <p><i>Owner:</i> Head of IT</p>

3.	Low	Familiarisation with contractual requirements
----	-----	---

Finding and Implication	Proposed action	Agreed action (Date / Ownership)
<p>For the Northgate Contracts there are weekly, monthly and quarterly meetings to resolve and manage service issues.</p> <p>The IT Service Manager is managing service obligations effectively and referring any exceptions to senior management. There has not been any incident serious enough to require reference to the contract, but the Service Manager is familiar with its content, and our discussions indicated that senior management may not be familiar with it.</p> <p>A précis of the contract, with key requirements summarised, had been planned to be put in place but this has not yet been achieved. .</p>	<p>Management should familiarise themselves with the key elements of the contract to ensure that Northgate are meeting contractual obligations and that these are being monitored. This should certainly be performed as part of the preparation for the annual review of the contract.</p> <p>As part of the planning for the annual review, summarising key parts of the contract (the planned précis exercise) would be timely and provide a useful aide memoire going forward.</p>	<p><i>Agreed action</i> Many of the provisions in the contract are well understood by ICO management, The new ICO/Northgate contract draws very heavily on the previous contract with Capita. The Contract Manager and Service Delivery Manager both worked on developing the contract and the procurement of Northgate. As recommended the opportunity of the annual contract will be used to develop a contract précis.</p> <p><i>Date Effective:</i> 31 July 2014</p> <p><i>Owner:</i> Head of IT</p>

## 2.2 Contract review points

4.	Low	Annual review for SCC contracts
----	-----	---------------------------------

Finding and Implication	Proposed action	Agreed action (Date / Ownership)
An annual review process is in place for the two major contracts (with Northgate). There is however no formal annual review currently scheduled for the SCC Contract.	Management should schedule a formal annual review with SCC in order for both parties to discuss contract performance, re-negotiate costs and charges and to propose any contractual changes.	<p><i>Agreed action.</i> The SCC contracts come under the Sprint II framework, scope for change is therefore limited. Holding regular (six monthly) contract reviews, as identified in finding 2, is considered sufficient opportunity to identify and discuss any contract changes. No further action proposed.</p> <p><i>Date Effective:</i> 27 May 2014</p> <p><i>Owner:</i> Head of IT</p>

## 2.3 Transition arrangements

5.	Medium	Deliverables from Northgate "transition plan"
----	--------	---

  

Finding and Implication	Proposed action	Agreed action (Date / Ownership)
<p>The transition plan from Northgate, was established not only to handle the immediate transfer of responsibilities from Capita, but also to provide a number of other deliverables over a longer period of time. There are a number of deliverables which are currently outstanding, so the transition plan remains incomplete at this stage. The key outstanding matters are:</p> <ol style="list-style-type: none"> <li>1) Establishing a baseline of IT and systems performance that allows both the ICO and Northgate to identify potential capacity or performance issues. While the ICO and Northgate are currently working collaboratively when any performance issues are identified, to establish the cause of any issues, a baseline is still required</li> <li>2) The transition from Capita to Northgate was also planned to deliver an IT future roadmap that would provide the ICO with a long term plan for potential changes or upgrades to the IT infrastructure.</li> <li>3) An exit plan is expected to be delivered which documents what would need to be taken on by a new supplier, and provides an overview of how such a transition would be achieved.</li> </ol> <p>While there is a service catalogue in place, it does not currently hold sufficient details on the services in place. A comprehensive service catalogue would provide a key reference point for both the ICO and Northgate to support each of these areas. In particular, although there are no indications that a change of contractor is expected, and the Northgate contract runs until mid 2016, the ICO would find moving to another supplier more challenging without these deliverables. .</p>	<p>Management are already dealing with this issue and there is an expectation that all transition activity will be completed prior to the contract's anniversary in July 2014.</p> <p>We would suggest a formal timetable is established for each of these deliverables,</p>	<p><i>Agreed action</i> Actions and progress are actively being tracked and are reviewed in the Monthly Service Meeting. At the meeting held on 20 May 2014, four topics were agreed as complete (Subcontractor Management, Remote Support, Change Management and Disaster Recovery). The remaining areas are System Monitoring / Management, Documentation &amp; Completion of Service Descriptions and Contract Schedules are to be completed by the contact anniversary on 9 July 2014</p> <p><i>Date Effective:</i> 27 May 2014</p> <p><i>Owner:</i> Head of IT</p>

## A Internal audit approach

### Approach

Our role as internal auditor to a Public Body is to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance processes, by measuring and evaluating their effectiveness in achieving the organisation's agreed strategic objectives.

Our audit was carried out in accordance with the guidance contained within the Government's Internal Audit Standards (2013) and the Auditing Practices Board's 'Guidance for Internal Auditors'. We also had regard to the Institute of Internal Auditors' guidance on risk based internal auditing (2005). In addition, we comply in all material respects with other Government guidance applicable to Public Bodies and have had regard to the HM Treasury guidelines on effective risk management (the 'Orange Book').

As part of our 2013-14 Audit Plan, we agreed with the Audit Committee and management that we should carry out a review of the ICO's arrangements for managing IT services now delivered by a number of suppliers, to further inform our on-going understanding of the ICO's key internal control activities.

Our aim in completing this audit was to ensure that the ICO has appropriate arrangements in place to identify, manage and report on risk.

We achieved our audit objectives by:

- meeting with key staff to gain an understanding of the arrangements in place to manage the relationship with suppliers, measure and manage their performance and the quality of delivery of IT services to the ICO;
- identifying the key risks, management controls to mitigate these risks and evaluating the effectiveness of the governance controls over IT service provision; and
- reviewing key documents that support the above processes.

The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of internal control arrangements.

### Responsibilities

The Information Commissioner acts through his Board of Management and the Information Commissioner's Office ("ICO") discharges his obligations. Therefore references to the Information Commissioner and the ICO in this report relate to one and the same party.

It is the responsibility of the Information Commissioner to ensure that the ICO has adequate and effective risk management, control and governance processes.

HM Treasury's Corporate Governance in Central Government Departments (2011) states that boards of Public Bodies should determine the nature and extent of the significant risks it is willing to take in

achieving its strategic objectives. The Board should therefore maintain sound risk management and internal control systems and should establish formal and transparent arrangements for considering how they should apply the corporate reporting and risk management and internal control principles and for maintaining an appropriate relationship with the organisation's auditors.

Please refer to our letter of engagement for full details of responsibilities and other terms and conditions.

### Scope

The objective of the review was to establish that third-party services are being delivered according to contractual requirements and so meet the ICO requirements. The focus of review was on the following risks:

- operational and legal requirements were not being met (as a minimum); they were not monitored and corrective action is not being taken when appropriate, leading to poor performance by suppliers;
- definition of the following areas were unclear:
  1. services being provided including those relating to security, availability and service recovery
  2. responsibilities and accountabilities of suppliers and ICO staff;
  3. ownership of physical assets, responsibility for their maintenance and transfer at contract termination;
  4. software licensing arrangements including for renewal (if applicable) and transfer at contract termination (if allowed);
  5. contract breach or the remedies established should such a breach occur;
- risks and rewards for either party were not defined and agreed, and/or the link between service performance and cost was not made sufficiently clear;
- there were inadequate mechanisms for establishing, agreeing, implementing and paying for contractual changes;

- no review points (either time or event driven) had been built in to the contract, so preventing either party from re-negotiating costs or services; and
- provisions were not in place to allow for smooth transition from a current supplier to a new supplier, leading to disagreement between the ICO and the supplier, and uncertainty over transition (such as transfer of assets and impact on people).

### Additional information

#### Client staff

The following staff were consulted as part of this review:

- Daniel Benjamin – Director of Corporate Services
- Dave Wells – Head of IT
- Angela Muston – Contract Manager
- John Rackstraw – IT Service Manager
- Simon Ebbitt – Information Security Manager
- Vipul Patel – Account Director, Northgate
- Les Smith – Interim Client Service Manager, Northgate
- Jill Sanderson – Service Manager, Northgate

## Documents received

The following documents were received during the course of this audit:

- Northgate Contract - Hosting and Systems Management
- Northgate Contract – Applications and desktop management
- ICO Terms of Reference for Partnership Governance v 3 0
- Northgate - weekly service review - 20140410 10042014
- Northgate - Weekly Service Review – 20140424
- Northgate - Weekly service review – 20140508
- Northgate - Weekly service review -20140501
- Meeting minutes.Jan 2014.VPamend – Agreed
- MSB Minutes.Feb 2014
- MSB Minutes.March 2014
- MSB Minutes April 2014
- QCB Minutes. Oct 2013 – Agreed
- QCB Meeting Minutes - April 2014.v1 – Draft
- CCN-001 Change Control Procedure Apps Desktop
- Appendix to CCN-001 Apps Desktop
- Appendix to CCN-001 Apps Desktop
- Northgate BMC Comments\_AK (SCC advice)
- Danwood- metering readings – 20140414
- Danwood - Service Review report - Jan - Mar 14
- Danwood - Service review – 20140115
- Danwood - Service review report - Sept - Dec 2013
- Danwood - Service review - 20140408

## Locations

We visited The Information Commissioner's Office, Wilmslow only for this review.

## B Overall assessment and audit issues ratings

### Overall assessment

Rating	Description
<b>Red</b>	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which should be raised with Senior Management and the Audit Committee at the earliest opportunity.
<b>Amber</b>	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which require the attention of management to resolve and report on progress in line with current follow up processes.
<b>Green</b>	We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.

### Audit issue rating

Within each report, every audit issue is given a rating. This is summarised in the table below.

Rating	Description	Features
<b>High</b>	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	<ul style="list-style-type: none"> <li>• Key control not designed or operating effectively</li> <li>• Potential for fraud identified</li> <li>• Non compliance with key procedures / standards</li> <li>• Non compliance with regulation</li> </ul>
<b>Medium</b>	Important findings that are to be resolved by line management.	<ul style="list-style-type: none"> <li>• Impact is contained within the department and compensating controls would detect errors</li> <li>• Possibility for fraud exists</li> <li>• Control failures identified but not in key controls</li> <li>• Non compliance with procedures / standards (but not resulting in key control failure)</li> </ul>
<b>Low</b>	Findings that identify non-compliance with established procedures.	<ul style="list-style-type: none"> <li>• Minor control weakness</li> <li>• Minor non compliance with procedures / standards</li> </ul>
<b>Improvement</b>	Items requiring no action but which may be of interest to management or best practice advice	<ul style="list-style-type: none"> <li>• Information for department management</li> <li>• Control operating but not necessarily in accordance with best practice</li> </ul>



© 2014 Grant Thornton UK LLP. All rights reserved.

“Grant Thornton” refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions.

**[grant-thornton.co.uk](http://grant-thornton.co.uk)**